Privacy, HIPAA, and Information Sharing
Fact Sheet

A publication of the National Indian Child Welfare Association

October 2014

How to Make HIPAA Your Friend

A significant tool of collaborative health care is the ability to share health information for the best outcome of the individual. This sharing transaction is sighted as confusing, controversial, and full of roadblocks to insure meeting federal regulations established to protect health information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191

- Established the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule").
- Addresses the use and disclosure of individuals' health information (called "protected health information") by organizations subject to the Privacy Rule (such organizations are called "covered entities") which include:
  - Individual and group plans that provide or pay the cost of medical care.
  - Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions (claims, benefit eligibility inquiries, referral authorization requests, or other transactions under the HIPAA Transactions Rule).[i]
- Addresses standards for individuals' privacy rights to understand and control how their health information is used.[ii]

For Consumers

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates (a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information) and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes.[iii]

What is Important to Provide Collaborative Care for Covered Entities and Business Associates

One of the major barriers to inter-agency collaboration is the misunderstanding of HIPAA regulations and how information can be shared across agencies. If you know the rules and special criteria, it can serve as an essential lifeline to a collaborative health care approach.

General Principle for Uses and Disclosures[iv]

Basic Principle	Required Disclosures
A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.	A covered entity must disclose protected health information in only two situations: (1) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (2) to United States Department of Health and Human Services when it is undertaking a compliance investigation or review, or enforcement action.

[i] Description and explanation of covered entities website www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

[ii] Summary of the HIPAA privacy rule. (n.d.). *Health information policy*. Retrieved from U.S. Department of Health and Human Services website www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

[iii] Understanding health information privacy. (n.d.). *Health information policy*. Retrieved from U.S. Department of Health and Human Services website www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[iv] Summary of the HIPAA privacy rule. (n.d.). *Health information policy*. Retrieved from U.S. Department of Health and Human Services website www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Privacy, HIPAA, and Information Sharing

There are six permitted uses and disclosures without an individual's authorization for the following purposes or situations:

1. To the individual (unless required for access or accounting of disclosures)
2. Treatment, payment, and health care operations
3. Opportunity to agree or object (informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object)
4. Incident to an otherwise permitted use and disclosure (the Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated)
5. Public interest and benefit activities (the Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes)[v]
6. Limited data set for the purposes of research, public health, or health care operations

While all of the above permitted use and disclosures are important, the criteria we are going to pay most attention to is likely going to be "treatment, payment, health care operations."

A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[vi] A covered entity may voluntarily choose, but is not required, to obtain the individual's consent for it to use and disclose information about him or her for treatment, payment, and health care operations. A covered entity that chooses to have a consent process has complete discretion under the Privacy Rule to design a process that works best for its business and consumers. The table below details the specific activities that meet the "use & disclose" disclosure criteria.

Treatment, Payment, and Health Care Operations Activities	Meets Permitted Use & Disclosure Criteria
Treatment activities of any health care provider: • The provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another	✓
Payment activities of another covered entity and of any health care providers: • Activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual	✓
Health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities: • (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity	✓
Covered entities which have or had a relationship with the individual and the protected health information pertains to the relationship[vii] • The relationship relates to one of the three activities described above	✓

[v] More information on the 12 national priority purposes can be found on pages 6-9 at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[vi] *Uses and disclosers of protected health information*. 45 C.F.R. § 164.502(a)(1).

[vii] Uses and disclosures for treatment, payment, and health care operations. (n.d.). *Health information policy*. Retrieved from U.S. Department of Health and Human Services website www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Memoranda of Understanding

A collaborative group of health care providers may choose to develop a memorandum of understanding (MOU) to specifically spell out the scope of the relationship, nature of sharing, and rules of confidentiality as they relate to HIPAA. An MOU can be a useful tool for care coordination and communicating with expert consultation to wrap care around an individual. Procedurally, this task could have a number of roadblocks unless specific elements, especially client flow, are clearly described in advance of the care coordination. The MOU serves as the vehicle for establishing the requirements of the agreement. In this respect it can be used in the following ways:

- Delineate client flow
- Specify services to be provided by a provider agency to clients
- Specify the type of clients appropriate for each agency agreeing to the MOU and how referrals should be made
- Facilitate communication by defining a process for regular meetings, phone contact, or data exchange.
- Protect both parties against differing interpretations of expectations by either party, by spelling out details of the relationship
- Eliminate barriers by defining new or altered procedures for clients
- Enhance the status of the case management agency in the community through formalized relationships with established or influential agencies
- Clearly delineate responsibilities of each entity
- Transfer authority to perform a mandated function from one agency to another or from one level of government to another.[viii]

Types of Data Sharing Agreements

There are two types of frequently used data sharing agreements:

I. Requesting personally identifiable information (PII), protected health information (PHI) and/or limited data set (LDS)

II. Requesting de-identifiable data.[ix]

	Summary	Terms	Data Included/Excluded
Type I	Where PII, PHI, and LDS is requested	PII refers to information that can be used to distinguish or trace an individual's identity. PHI refers to individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records. LDS refers to PHI that excludes 16 direct identifiers listed below in the Privacy Rule of the individual or of relatives, employers, or household members of the individual.	LDS exclusions: 1. Names 2. Postal address information, other than town or city, state, and zip code 3. Telephone numbers 4. Fax numbers 5. Email addresses 6. Social security numbers 7. Medical record numbers 8. Health plan beneficiary numbers 9. Account numbers 10. Certificate/license numbers 11. Vehicle identifiers and serial numbers, including license plate numbers 12. Device identifiers and serial numbers 13. Web Universal Resource Locators (URLs) 14. Internet protocol (IP) address numbers 15. Biometric identifiers, including finger and voiceprints 16. Full-face photographic images and comparable images

The summary, terms, and included/excluded data for Type II is listed on the next page.

[viii] Johnson, M. & Sterthous, L. (1982). *A guide to memorandum of understanding negotiation and development*. Philadelphia, PA: Temple University. Retrieved at http://aspe.hhs.gov/daltcp/reports/mouguide.htm

[ix] U.S. Department of Defense. (2003). *Directive 6025.18-R: Health information privacy regulation*. Washington, D.C.: U.S. Department of Defense. Retrieved at www.dtic.mil/whs/directives/corres/pdf/602518r.pdf; U.S. Department of Defense. (2007). *Directive 5400.11-R: Department of Defense privacy program*. Washington, D.C.: U.S. Department of Defense. Retrieved at www.dtic.mil/whs/directives/corres/pdf/540011r.pdf

Privacy, HIPAA, and Information Sharing
Fact Sheet

A publication of the National Indian Child Welfare Association

	Summary	Terms	Data Included/Excluded
Type 2	Where PHI is requested and will be de-identified after it is disclosed.	PHI refers to individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records. De-identified data refers to health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.	Methods of de-identifying data include **statistical method** and **safe harbor method**. **Statistical Method**: A qualified statistician or scientific expert concludes, through the use of accepted analytic techniques, that the risk the information could be used alone, or in combination with other reasonably available information, to identify the subject is very small. **Safe Harbor Method**: Removal of 18 identifiers of the individual or of relatives, employers, or household members of the individual. 1. Names 2. All geographic subdivisions smaller than a state 3. All elements of dates (except year) directly related to an individual 4. Telephone numbers 5. Fax numbers 6. Email addresses 7. Social security numbers 8. Medical record numbers 9. Health plan beneficiary numbers 10. Account numbers 11. Certificate or license numbers 12. Vehicle identifiers and serial numbers, including license plate numbers 13. Device identifiers and serial numbers 14. Web URLs 15. IP address 16. Biometric identifiers, including fingerprints and voice prints 17. Full-face photographs and comparable images 18. Any unique, identifying number, characteristic or code, except as permitted for re-identification under HIPAA

A Good Start

HIPAA regulations are indeed meant to protect private health information especially in era of electronic transmission of health care data. The regulations are not meant to be a hindrance but rather to offer guidance and direction on how best to protect individuals' information and provide comprehensive care. The resources in this fact sheet are meant to offer a better understanding of HIPAA regulations and how to use them collaboratively in the care of individuals.

NICWA

National Indian Child Welfare Association

This fact sheet was published by the National Indian Child Welfare Association (NICWA) with support from the Child, Adolescent and Family Branch (CAFB), Center for Mental Health Services (CMHS), Substance Abuse and Mental Health Services Administration (SAMHSA). The content of this publication does not necessarily reflect the views, opinions, or policies of CAFB, CMHS, SAMHSA, or the Department of Health and Human Services.